STATE OF CALIFORNIA
DEPARTMENT OF INSURANCE
45 Fremont Street, 21st Floor
San Francisco, California 94105

RH01018269 **October 2, 2002**

FINAL STATEMENT OF REASONS AND UPDATED INFORMATIVE DIGEST

PRIVACY OF PERSONAL INFORMATION

INTRODUCTION AND UPDATED INFORMATIVE DIGEST

California Insurance Commissioner Harry W. Low has adopted Title 10, Sections 2689.1 -- 2689.24, California Code of Regulations, regarding privacy of information gathered by licensees in connection with insurance transactions.

The purpose of these regulations is to implement, interpret and make specific the provisions of California Insurance Code, Division 1, Part 2, Chapter 1, Article 6.6, Sections 791 -- 791.27 and the privacy provisions of the federal Gramm-Leach-Bliley Financial Services Modernization Act[1] (GLBA), 15 U.S.C., Subchapter I, Sections 6801 -- 6810.

California Insurance Code (CIC) Sections 791 -- 791.27, the Insurance Information and Privacy Protection Act enacted in 1980, establish standards for the collection, use, and disclosure of information gathered in connection with insurance transactions. This legislation adopted the National Association of Insurance Commissioners' (NAIC) 1982 model legislation, developed with input from state regulators and representatives of industry, producers and consumers to facilitate uniform privacy standards among states. Regulations were not necessary to implement that law when it was enacted.

Title V of GLBA (15 U.S.C. Sections 6801 -- 6810) requires various federal agencies and state insurance authorities to enact regulations respecting the privacy of customers and protecting the security and confidentiality of nonpublic personal information. Federal agencies have adopted implementing regulations for financial institutions subject to the jurisdiction of federal regulators. GLBA expressly permits states to enact privacy protections greater than those required by GLBA or by federal regulations.

Currently, there are no regulations that govern the collection, use, disclosure, and safeguarding of information under Sections 791 -- 791.27 of the Insurance Code. (In 2002, the NAIC adopted model safeguarding regulations, which are incorporated herein.) The lack of regulations has led to some confusion on the part of licensees regarding their obligations under California and federal law. These proposed regulations are intended to clarify implementation of the privacy protections set forth in the Insurance Code and to comply with the GLBA mandate, consistent with the public policy of providing maximum privacy protection permitted under these laws.

[1] P.L. 106-102, signed November 12, 1999.

SPECIFIC PURPOSE OF THE REGULATONS AND NECESSITY

The specific purpose of each regulation and the rationale for the Commissioner's determination that each regulation is reasonably necessary to carry out the purpose for which it is proposed is set forth below.

Article I: General Provisions

Section 2689.1 Authority and Purpose

Section 2689.1 provides authority for the promulgation of these regulations and clarifies that these regulations are intended to implement provisions of CIC §§791 -- 791.27 and to comply with the GLBA mandate. The rationale for adopting this regulation is to clearly indicate to the public the legal authority for this rulemaking and the provisions of the Insurance Code and Gramm-Leach-Bliley which are being implemented.

Section 2689.2 Scope

Section 2689.2 clarifies that these regulations apply to personal information gathered by certain licensees about policyholders, claimants and beneficiaries of insurance products or services used primarily for personal, family, or household purposes. Adopting this regulation is necessary to set forth clearly the persons and circumstances to which the regulations apply to assist affected persons in understanding provisions of the statute and regulations to ensure compliance.

Section 2689.3 Disclosure of Information

Section 2689.3 specifies that personal information shall not be disclosed in a manner not permitted by California law or these regulations. Adoption of this regulation is necessary to reiterate and make clear the obligations imposed on licensees.

Section 2689.4 Definitions

Section 2689.4 defines several key terms referred to in these regulations that are not defined in CIC §§791 -- 791.27 and might otherwise be unclear to affected persons. Adoption of this regulation is necessary for the public to understand provisions of the statutes and regulations.

Section 2689.4(a) requires that notices of information practices be "clear and conspicuous." This section generally adopts the same standards for a "clear and conspicuous" notice as those in related regulations adopted by the federal agencies. Additionally, the regulation provides that a notice is reasonably understandable if it achieves a minimum Flesch Score of 50, which is an objective standard for determining that notices should be understandable by those with a high school education. This recognizes both the importance of ensuring that privacy notices will be understood by most readers and the fact that the privacy notices contain technical information and must communicate various legal requirements.

This section also provides that if a notice is on the back or inside of a multi-page form, it should be accompanied by a prominent notice on the front of the form directing the reader's attention to the privacy notice and where it may be found. This recognizes that privacy notices may be included with other documents, but also ensures that consumers are alerted to the privacy notice.

Section 2689.4(a) also sets forth requirements for notices on web sites, in recognition of the fact that many consumers now conduct business on the web and will therefore receive privacy notices via the web site.

The rationale for this regulation is to achieve consistency and uniformity in privacy standards between California and federal law. The added standards are reasonably necessary to ensure that consumers will understand a licensee's privacy notices.

Section 2689.4(b) defines "collect" consistent with the definition in federal regulations adopted by various federal agencies. The Insurance Code and GLBA establish standards for the collection of nonpublic personal information in connection with insurance transactions. The rationale for this regulation is to assist interested persons in understanding these provisions and to achieve uniformity in privacy standards between California and federal law.

Section 2689.4(c) defines "consumer" in terms similar to GLBA except that this regulation includes claimants and beneficiaries as examples of consumers not included in GLBA because GLBA focused on financial institutions, not insurance entities. This is an important definition because it clarifies the scope of the regulations. The rationale for adoption of this regulation is to assist licensees in understanding the statutes and regulations to ensure compliance.

Section 2689.4(d) defines "customer" in terms of a continuing relationship and provides examples of when a consumer is or is not a customer, as do the federal regulations adopted by applicable federal agencies. GLBA requires that licensees provide notice of their information practices at the time of establishing a customer relationship and then annually. This section provides that if a consumer's last known address is deemed invalid, and if the consumer has not opted out, the licensee shall remove the consumer's name from specified marketing lists. This requirement ensures that information is not disclosed about a consumer who does not receive a privacy notice and therefore does not opt out. This regulation is necessary to clarify who is and who is not a customer so that affected persons are knowledgeable about their rights and obligations.

Section 2689.4(e) defines "financial institutions" and Section 2689.4(f) defines "financial product or service" according to similar standards in GLBA and federal regulations. Since the Insurance Code focuses on licensees subject to the Insurance Commissioner's jurisdiction, it does not define these terms. Consequently, the terms may be unclear to licensees. However, GLBA imposes privacy obligations on "financial institutions," including insurers. The rationale for this regulation is to assist affected persons in understanding the applicability and scope of relevant privacy laws and achieve consistency and uniformity between California and federal law.

Section 2689.4(g) defines "nonaffiliated third party" consistent with standards in GLBA and federal regulations adopted by applicable federal agencies. CIC §§791 -- 791.27 and GLBA establish required standards for notice and disclosures of nonpublic personal information to affiliated and nonaffiliated third parties. The distinction is significant and this regulation clarifies the distinction so that consumers and licensees understand their rights and obligations.

The rationale for this regulation is to achieve uniformity in privacy standards between California and federal law.

Section 2689.4(h) defines "nonpublic personal financial information" in the same manner as it is defined in the NAIC model regulation regarding privacy of consumer financial and health information, adopted in September 2000. The definition is designed, to the extent possible, to ensure uniformity in the definition of nonpublic personal financial information.

Section 2689.4(i) defines "nonpublic personal information" to include both nonpublic personal financial information and medical record information, similar to the NAIC 2000 model regulations and the federal regulations adopted by applicable federal agencies. Nonpublic personal information includes lists derived using information not publicly available, information obtained through an internet cookie, information from a consumer report, and specified information about individuals associated with a business entity. This regulation specifies the type of information that is covered by these privacy provisions so that affected persons understand their rights and obligations. The rationale for this regulation is to facilitate uniformity of privacy standards between California and federal law, to the extent feasible.

Sections 2689.4(j) and (k) define "opt-in" and "opt-out" as those terms have been used in the context of the GLBA privacy requirements. These definitions were added at the suggestion of consumer groups to ensure that those reading the regulations understand the terms in a similar fashion.

Section 2689.4(l) defines "ownership of voting securities" similar to the federal regulations for uniformity and consistency purposes.

Section 2689.4(m) defines "publicly available information" in terms similar to the federal regulations adopted by the applicable federal agencies and describes when a licensee has a reasonable basis to believe that information is lawfully made available. This regulation allows affected persons to understand their rights and obligations and to facilitate uniformity of privacy standards, to the extent feasible.

Article II: Privacy Notices; Opt Out Notices for Nonpublic Personal Financial Information

Section 2689.5 Initial Privacy Notice

Section 2689.5 provides that licensees shall provide specified clear and conspicuous privacy notices to customers, claimants, and beneficiaries. It sets forth standards under which an initial privacy notice may be delivered within a reasonable time after a customer relationship is established, paralleling federal regulations applicable for federal agencies. It provides that licensees may provide required notices in a single combined notice or in separate notices. The purpose of this regulation is to clarify procedures for the initial privacy notice so that licensees understand their obligations to ensure compliance. Adoption of this regulation is necessary to comply with the GLBA mandate and, to the extent feasible, to achieve uniformity of privacy standards between California and federal law and regulations.

Section 2689.6 Annual Privacy Notice
Section 2689.6 adopts an annual notice requirement for customers. CIC §791.04 provides that a licensee meets requirements for notice of information practices, in the case of a policy renewal, if notice is delivered within the previous 24 months. However, GLBA (15 U.S.C. Section 6803) requires annual notice to a customer, as defined in federal regulations. Since the federal standard of annual notice is stricter, federal law supersedes. The rationale for this regulation is to conform to the mandated federal standard.

This regulation additionally permits a licensee to provide the CIC §791.04 notice and the GLBA notice either as separate notices or in a single combined notice, if specified requirements are met. The rational for this provision is to allow licensees to use standardized notices, supplemented by a specified California notice, thus allowing for countrywide consistency and uniformity to the extent possible.

Section 2689.7 Information to be Included in Privacy Notices
Section 2689.7 clarifies information requirements for privacy notices by adopting similar standards contained in federal regulations adopted by applicable federal agencies. Often consumers are unaware of the information that is collected about them in connection with insurance transactions and do not know the uses made of the information collected. Without such information, they cannot make informed choices based on privacy concerns they may have. The purpose of this regulation is to assist the consumer in obtaining such information. The rationale for this regulation is to achieve uniformity between California and federal law, to the extent feasible. For clarification, this section also makes clear that written authorization before a licensee discloses nonpublic personal information must comply with standards set forth in CIC §791.13(a). And at the request of consumer groups, this section specifies that, if a financial institution seeks to disclose information to an affiliate for marketing purposes, its notice shall also indicate that a customer has no legal right to opt-out of that disclosure. The rationale is to make it clear to customers that the law allows for this information sharing. This section also provides that abbreviated notices shall be clear and conspicuous (the same standard applicable to other notices) and set forth a reasonable means for consumers to obtain the more detailed notice.

Section 2689.8 Form of Opt Out Notices and Opt Out Methods
Section 2689.8 clarifies opt out procedures and information requirements to be followed when a licensee is required to provide an opt out notice. CIC §791.13 sets forth the general rule that a licensee is prohibited from disclosing a consumer's nonpublic personal information without prior written authorization, subject to certain exceptions. One of the exceptions, CIC §791.13(k), permits disclosure to a nonaffiliated third party for marketing purposes, but requires that a consumer be given an opportunity to indicate he or she does not want personal financial information disclosed (opt out) and has not so indicated. The statute does not specify opt out procedures. However, federal regulations adopted by applicable federal agencies set forth standards for a clear and conspicuous notice that explains the right to opt out, provide examples of opt out methods, and set forth procedures for handling an opt out direction by joint consumers. This regulation adopts the federal standards. The purpose of this regulation is to make clear how a consumer may exercise the right to opt out in applicable circumstances. Adoption of this regulation is necessary to achieve uniformity in privacy standards between California and federal law. This regulation provides that the notice must appropriately highlight the purpose of the

notice so consumers do not inadvertently overlook it. For the same reason, if the opt out notice is mailed with information that is not a bill or renewal offer, it must be the first page of the mailing. The financial institution must provide a simple and cost-free method for consumers to opt-out so that exercising this right does not come at an additional financial or other cost to them.

Like the new NAIC model, this regulation provides that an agent who "shops" a policy at renewal must so advise the policyholder and allow him or her the opportunity to opt out. This requirement is necessary to allow policyholders, if they choose to do so, to prevent the sharing of their nonpublic personal financial information with other insurers to in order to obtain different coverage.

This regulation sets forth the treatment of joint policyholders, similar to the NAIC model. It provides that a financial institution shall provide consumers with at least 30 days to exercise their opt out rights before the financial institution shares marketing information with nonaffiliated third parties. This is a reasonable time for consumers to receive and review the notice and respond if they choose to do so, recognizing that consumers also have other matters to attend to.

Section 2689.9 Revised Privacy Notices
Section 2689.9 clarifies procedures for revised privacy notices. CIC §791.04 sets forth standards for notice of information practices but does not specifically set forth standards for revised notices. However, federal regulations applicable to federal agencies require a clear and conspicuous revised notice that accurately describes a licensee's information policies and practices and provides for a new opt out form when applicable. This regulation adopts similar standards.

Section 2689.10 Delivery of Notices
Section 2689.10 clarifies standards and provides examples of adequate methods to deliver privacy notices. CIC §791.04 requires notice of information practices but does not specify methods of delivery of notices. However, federal regulations adopted by applicable federal agencies set forth standards of reasonable expectation of delivery and provide examples of both reasonable and unreasonable expectations. This regulation adopts similar standards and examples to ensure that such notification reaches consumers. The rationale for this regulation is to achieve uniformity of privacy standards between California and federal law and regulations.

Article III: Limits on Disclosures of Medical Record Information

Section 2689.11 Disclosure of Medical Record Information
Section 2689.11 clarifies the limits and conditions on disclosure of nonpublic personal medical record information. CIC §791.13 requires a licensee to obtain prior written authorization before disclosing nonpublic personal information, defined in CIC §791.02(s) to include medical record information, subject to certain exceptions. Since GLBA was focused on financial institutions, GLBA is silent on the treatment of medical record information. The rationale for this regulation is to make clear the limits on disclosure of medical record information.

Article IV: Standards for Safeguarding Nonpublic Personal Information

Section 2689.12 General Provisions

GLBA (15 U.S.C. Sections 6801, 6805(b) and 6807) specifically requires the establishment of standards to safeguard nonpublic personal information. Section 2689.12 clarifies that the regulations in Article V are intended to establish procedures to develop and implement administrative, technical, and physical safeguards to ensure the security and confidentiality of nonpublic personal information. The section also sets forth procedures and actions which licensees may implement, as applicable, to comply with the safeguarding standards. The regulations are similar to the federal regulations promulgated by the applicable federal agencies and to the NAIC model safeguarding regulations. Adoption of this regulation is necessary to harmonize California law and the GLBA.

Section 2689.13 Definitions

Section 2689.13 defines "customer information systems" and "service provider" consistent with the definitions in the NAIC 2002 model, developed to track GLBA requirements for safeguarding nonpublic personal information. The purpose of defining these terms is to assist licensees in understanding the safeguarding requirements in these regulations. Adoption of this regulation is reasonably necessary to achieve consistency between states and uniformity between California law and federal law.

Section 2689.14 Information Security Program

Section 2689.14 clarifies the requirements of an information security program for licensees. CIC §§791 -- 791.27 and GLBA establish broad standards for safeguarding nonpublic personal information, but do not specify the process. These provisions require licensees to implement systems appropriate for the licensee. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.15 Objectives of Information Security Program

Section 2689.15 establishes similar objectives for an information security program as in GLBA. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.16 Assess Risk

Section 2689.16 implements the safeguarding process mandated by GLBA by setting forth examples by which a licensee may assess the threat of risk to the integrity of customer information and information systems. The standards parallel the standards set forth in the NAIC's 2002 model. Although CIC §§791 -- 791.27 and GLBA established standards for the safeguarding of nonpublic personal information, the statutes did not specify the process. This regulation implements, interprets and makes specific those provisions. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.17 Manage and Control Risk

Section 2689.17 implements the safeguarding process mandated by GLBA by setting forth examples by which a licensee may manage and control risks to the integrity of customer

information and information systems. The standards parallel the standards set forth in the NAIC's 2002 model. Although CIC §§791 -- 791.27 and GLBA established standards for the safeguarding of nonpublic personal information, the statutes did not specify the process. This regulation implements, interprets and makes specific those provisions. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.18 Service Providers
Section 2689.18 implements the safeguarding process mandated by GLBA by setting forth examples for a licensee to oversee service providers. The standards parallel the standards set forth in the NAIC's 2002 model. Although CIC §§791 -- 791.27 and GLBA established standards for the safeguarding of nonpublic personal information, the statutes did not specify the process. This regulation implements, interprets and makes specific those provisions. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.19 Adjust the Program
Section 2689.19 implements the safeguarding process mandated by GLBA by setting forth examples by which a licensee may monitor and adjust the information security program. The standards parallel the standards set forth in the NAIC's 2002 model. Although CIC §§791 -- 791.27 and GLBA established standards for the safeguarding of nonpublic personal information gathered in connection with insurance transactions, the statutes did not specify the process. This regulation implements, interprets and makes specific those provisions. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.20 Enforcement
CIC §§791 -- 791.27 and GLBA impose a number of obligations upon licensees. The Insurance Code and 15 U.S.C., Section 6805(6) authorize the Insurance Commissioner to enforce these obligations. The rationale for Section 2689.20 is to clarify that the Insurance Commissioner is responsible for audit compliance and enforcement of these standards and regulations, consistent with the statutes. This regulation is similar to the NAIC 2002 safeguarding model.

Article V: Additional Provisions

Section 2689.21 Protection of Fair Credit Reporting Act
Section 2689.21 clarifies that CIC §§791 -- 791.27 does not modify, limit, or supersede the operation of the federal Fair Credit Reporting Act (FCRA) (15 U.S.C. §§1681 et seq.). Since disclosures of certain information may give rise to obligations under FCRA, GLBA (15 U.S.C. Section 6806) expressly protects the operation of FCRA. This regulation adopts a similar standard. The rationale of this regulation is to achieve uniformity in privacy standards between California and federal law. This provision is similar to Section 22 of the 2000 NAIC model.

Section 2689.22 Nondiscrimination
Section 2689.22 clarifies that a licensee is prohibited from discriminating against a consumer for withholding disclosure authorization by denying the consumer an insurance product or service.

CIC §791.13 requires prior written authorization before disclosure of nonpublic personal information, setting forth certain exceptions, including the requirement of an opt out notice to consumers before disclosing information to nonaffiliated parties for marketing purposes. It does not specify consequences when a consumer does not provide authorization or exercises the option of opting out against disclosure. The rationale for this regulation is to protect the consumer's exercise of privacy rights. This section is similar to Section 23 in the 2000 NAIC model.

Section 2689.23 Severability
Section 2689.23 clarifies that each section of the regulations is severable. The rationale for this regulation is consistency with customary legal protections if a section or portion of a section or its applicability to any person or circumstance is held invalid by a court. This section is similar to Section 25 of the 2000 NAIC model.

Section 2689.24 Effective Date
Section 2689.24 specifies that the Insurance Commissioner intends the effective date of these regulations to be 120 days after filing with the Secretary of State. The rationale for this regulation is to allow a reasonable time for licensees to implement the applicable provisions of the regulations. Because CIC §§791 – 791.27 have been in effect since 1981, and the GLBA privacy provisions were signed in 1999, 120 days after filing with the Secretary of State allows sufficient time for licensees to implement the applicable regulations.

Appendix A-Sample Clauses
Appendix A provides sample clauses to assist licensees in drafting privacy notices, explaining a consumer's right to opt out of disclosures, and describing its practices to protect the confidentiality and security of customer information. These examples are simply intended to provide guidance to licensees, and they are similar to examples set forth in the 2000 NAIC model.

SUMMARY OF AND RESPONSE TO PUBLIC COMMENT
The Department's summary of and response to public comment is separately included in this rulemaking file and incorporated herein by this reference.

IDENTIFICATION OF STUDIES
The Commissioner has not relied upon technical, theoretical, or empirical studies or reports in proposing these regulations. However, the Commissioner has relied on the two NAIC models referenced in this Final Statement of Reasons.

SPECIFIC ACTIONS, PROCEDURES, TECHNOLOGIES OR EQUIPMENT
Adoption of these regulations would not mandate the use of specific technologies or equipment or prescribe specific actions or procedures.

ALTERNATIVES
As set forth in the responses to comments on the proposed regulations and elsewhere in this rulemaking file, the Commissioner has determined that no reasonable alternative exists to carry

out the purpose for which the regulations are proposed or would be as effective and less burdensome to affected private persons than the proposed regulations.

MANDATES

The regulations do not impose a mandate on local agencies or school districts.

ECONOMIC IMPACT ON BUSINESS

The Commissioner has determined that the proposed regulations will not have a significant adverse economic impact on businesses because licensees are required to comply with similar federal requirements set forth in the Gramm-Leach-Bliley Financial Services Modernization Act (15 U.S.C., Subchapter I) and with California's existing privacy laws. To the extent economic impacts are imposed on businesses, those impacts are necessary to ensure adequate privacy protections for Californians. The Commissioner has adopted many of the public comments to attempt to minimize the impact on business to the extent consistent with ensuring adequate privacy protections.

FORM 399

The Commissioner has determined that the changes made to the proposed regulations after issuance of the originally proposed regulation text do not have a fiscal impact to state agencies, local agencies and school districts or federal funding. Therefore, the Fiscal Impact Statement (Form 399), signed December 5, 2001, is still accurate.